Integrating QKD in Telecommunication Networks

V. Martín, D. Lancho, J. Martínez, D. Elkouss, A. Ciurana
Quantum Information and Computation Group
http://gcc.ls.fi.upm.es/

Outline

- Introduction
- Metropolitan and testbed networks
- Results
- Conclusions
- What's next?

Introduction

- QKD (Quantum Key Distribution) is a quantum cryptography application that enables two remote parties to exchange secret keys
- The security is guaranteed through a combination of information theory and the laws of physics
- Common use QKD protocols consist of three steps:
  - Key exchange
  - Key sifting
  - Key distillation:
    - Error correction
    - Privacy amplification

Introduction

- QKD (nowadays):
  - It is neither a cheap nor easy technology
  - From a commercial perspective, has not a broad market yet
  - The claimed level of security has still to be proven by general adoption
    - In practice, may differ from theoretical security
  - It is limited to point-to-point and in distance
    - Trusted repeaters → intermediate nodes from a third party (man in the middle)

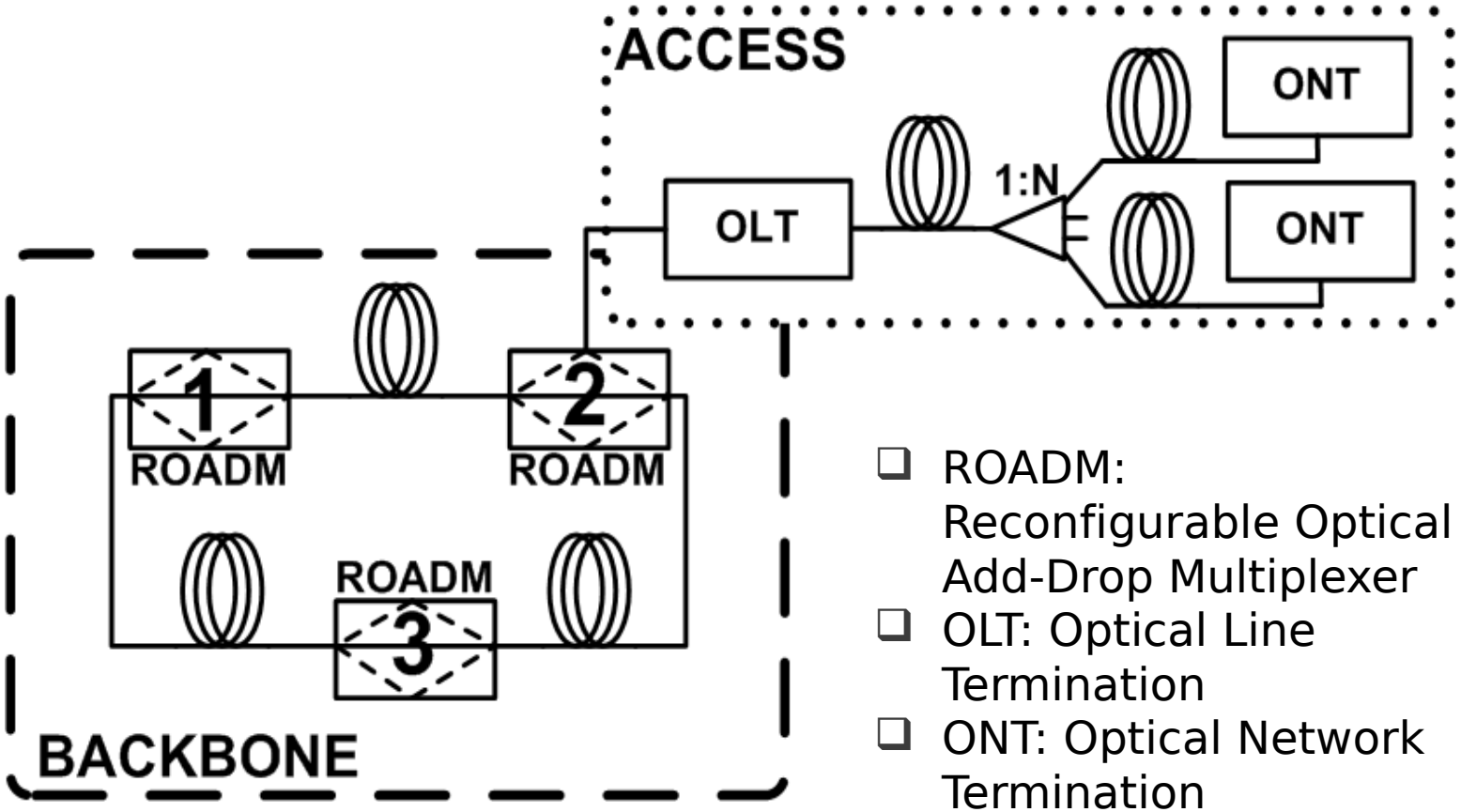
Introduction

- It seems unrealistic to think that a new and very expensive infrastructure is going to be created for QKD
- Solution → share the existing infrastructure:
  - Leverage costs
  - Deployed in a scalable way
  - More robustness
  - More confidentiality

Metropolitan and testbed networks

- Metro networks link the long haul network to the final users (within the same area)
  - Limited span, typically in the tens of Km
- The general trend is towards Passive Optical Networks (PONs)
  - No active components → simpler and cheaper
  - A transparent, non amplified, link among any two points of such a network is possible

Metropolitan and testbed networks



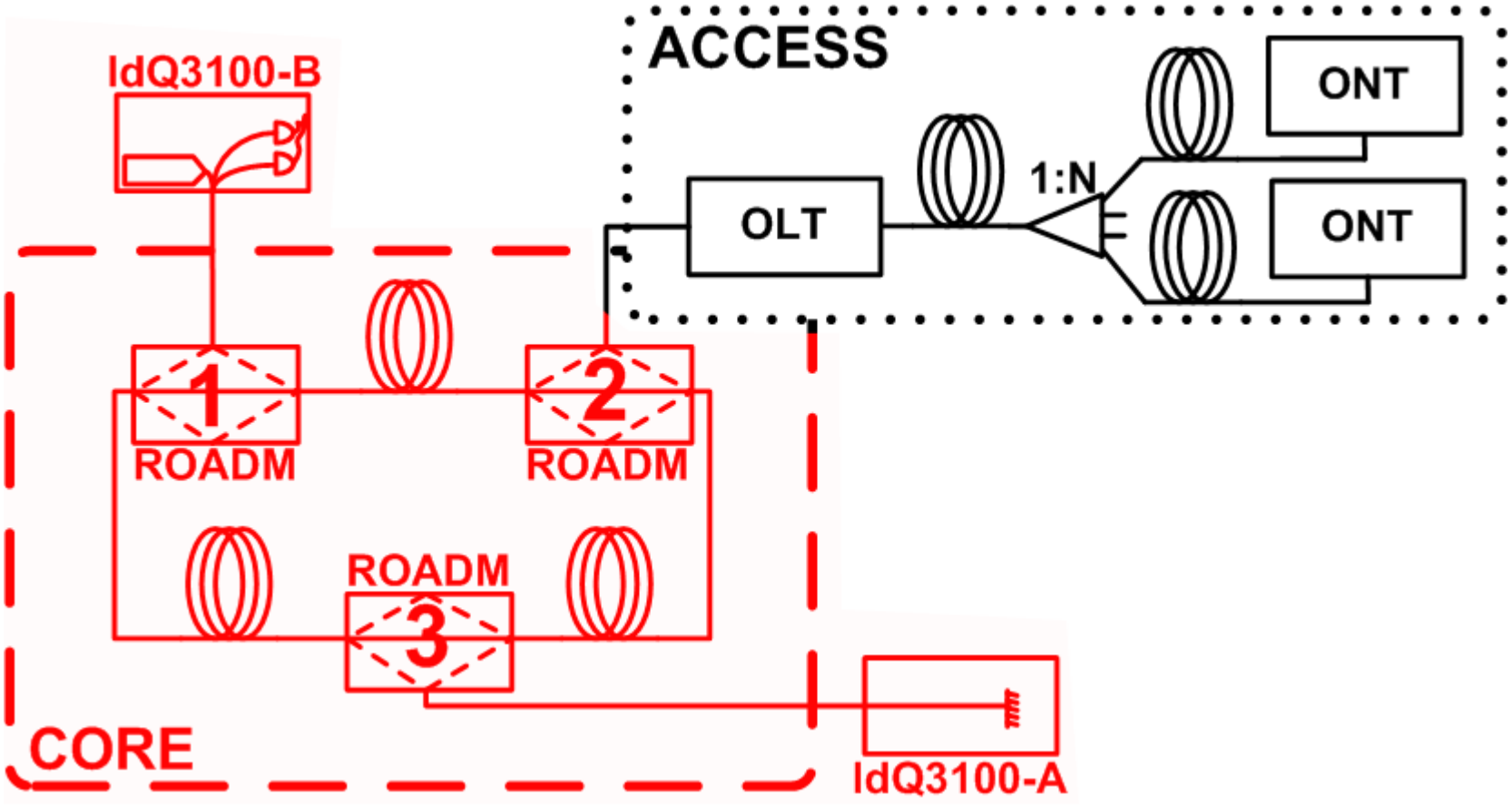
- ROADM: Reconfigurable Optical Add-Drop Multiplexer
- OLT: Optical Line Termination
- ONT: Optical Network Termination

- Patent (P200930742): *Sistema de integración de canales con información cuántica en redes de comunicaciones*

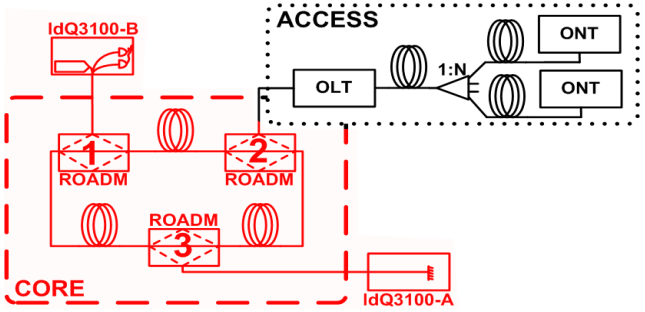
Metropolitan and testbed networks

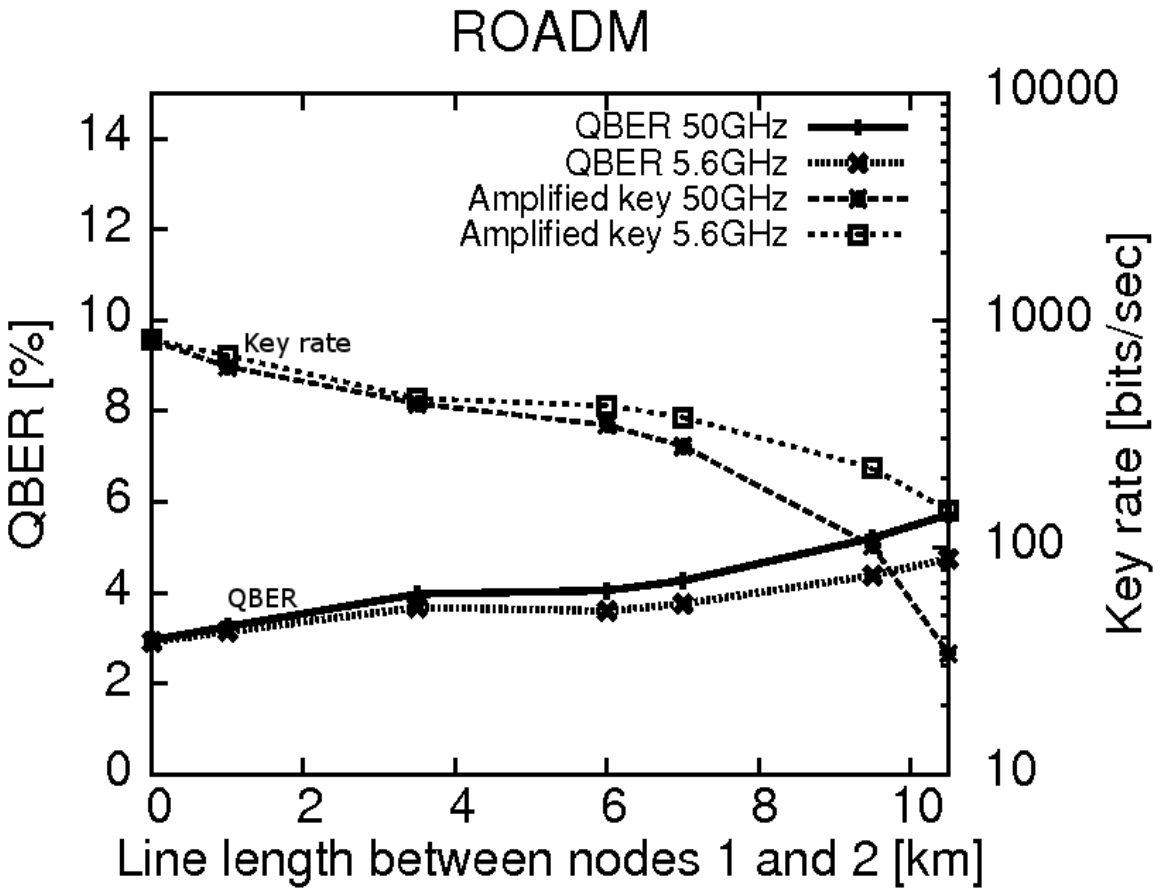
- Id Quantique Clavis (id3000, id3100)
  - Two way plug'n'play systems
  - Maximum key rate (min. loss and 0% error → only limited by detectors): 100Kbps
  - Maximum loss budget: ~12dB
- Protocol: BB84 with decoy states
- Error correction: LDPC codes

Results


IdQ3100-B
ACCESS
ONT
1:N
OLT
ONT
1
ROADM
2
ROADM
ROADM
3
CORE
IdQ3100-A

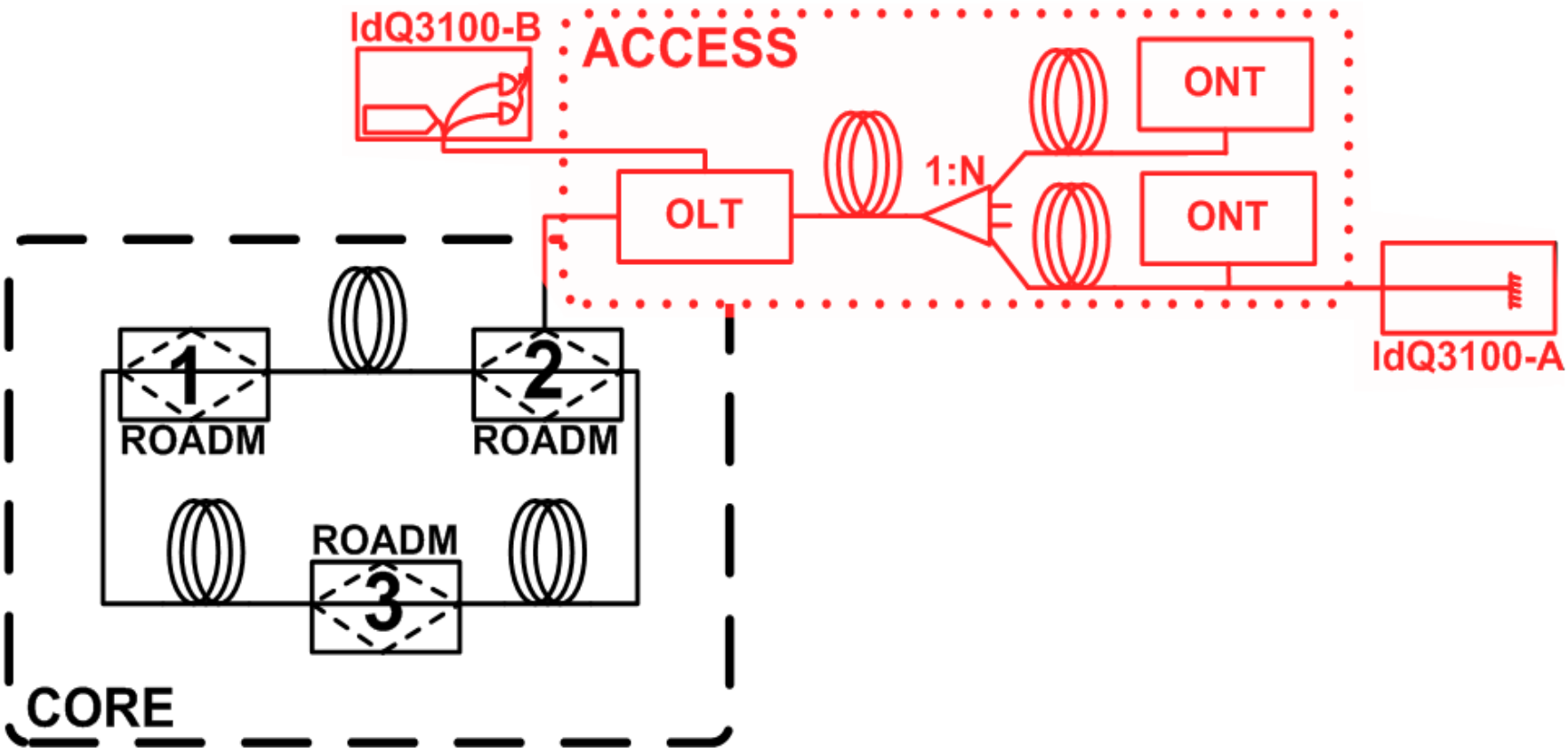
Results



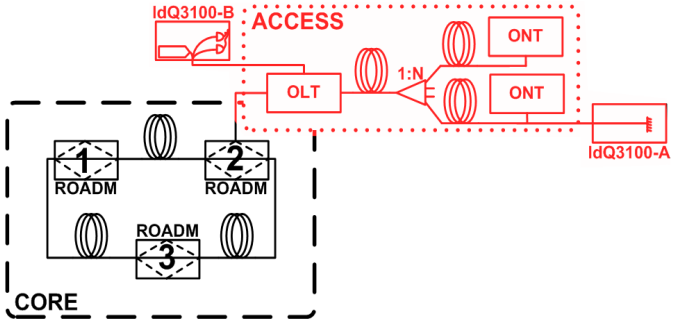


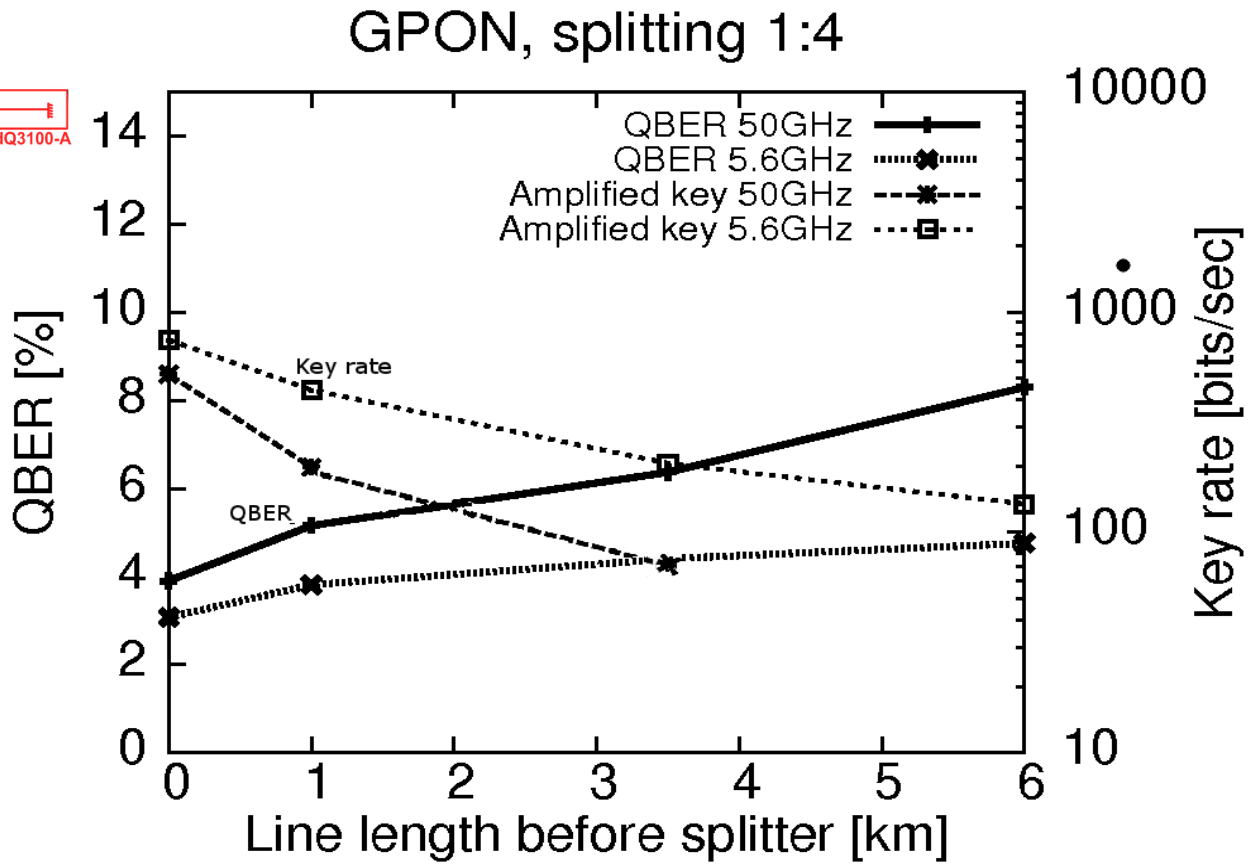
- Results exposed on QuantumComm 2009 (Naples, Italy) and UQCC 2010 (Tokyo, Japan)

Results


IdQ3100-B
ACCESS
ONT
1:N
OLT
ONT
IdQ3100-A
1
ROADM
2
ROADM
ROADM
3
CORE

Results





- *Paper: Efficient Reconciliation with Rate Adaptive Codes in Quantum Key Distribution* (QIC, 2010)
- Patent (P201030099): *Método y sistema de comunicaciones para la reconciliación de información para QKD mediante el uso de códigos*

Conclusions

- Even with the conditions of deployed commercial optical networks it is possible for a quantum channel and classical signals to multiplex in the fiber
- Major problems:
  - Losses from devices
  - Raman scattering
- Throughput is still enough to be used in a combined QKD/block cipher (like AES) with a much higher key refresh rate than that used nowadays

Conclusions

- It is necessary an effort by the Optical Devices' manufacturers:
  - Limit the total power in the shared lines
  - Use better detectors and lasers
    - to limit the power while being compliant with the standard budget loss
  - Improve the conventional devices: avoid unnecessary losses).
- Better QKD devices (budget loss > 30 dB) would allow to perform a key exchange among two points within a metro network, without the need of trusted repeaters

Conclusions

- Current Infrastructure is rapidly evolving → New technologies → More standards to be “QKD friendly”
  - *The Integration of QKD in Standard Optical Networks (draft)*
  - *Quantum Key Distribution: Application Interface (published)*
  - *Quantum Key Distribution: Security Specifications (published)*

What's next?

- Future experiments
  - Several quantum channels and classical channels.
    - Backbone
    - Access network
  - DWDM-PON
  - QKD on 1310nm
    - Less Raman scattering
    - Better detectors
    - More fiber losses (not one of our major problems)
  - Entangled photons with AIT (Austrian Institute Of Technology)

Thanks!

Quantum Information and Computation Group

Facultad de Informática – UPM

http://gcc.ls.fi.upm.es/
aciurana@fi.upm.es